Digital Signatures for Patient Documents Delivered via the WWW

Gary K. Allen, D.V.M., Ph.D.[1,2], David M. Witten II[2], Timothy B. Patrick, Ph.D.[2,3]
[1]Department of Veterinary Pathobiology, College of Veterinary Medicine,
[2]Integrated Technology Services, School of Medicine,
[3]School of Library and Informational Science, College of Education
University of Missouri, Columbia, Missouri

Background. The World Wide Web (WWW) is increasingly being used as a delivery platform for biomedical documents. Methods to implement data integrity policies are needed to ensure the correctness of information contained in these documents. Such policies are intended to ensure that data remain consistent with its source and to allow the identification of errors, duplications, omissions, and intentional alterations. Secure methods for authentication and validation of documents are particularly important. Digital signatures can be used to accomplish these tasks, and have been successfully applied in electronic mail and traditional networked computing environments. It is important to demonstrate the practical application of digital signatures in WWW-based medical document delivery systems.

The Missouri Kidney Program (MoKP) is dedicated to meeting the medical, educational, and psychosocial needs of eligible Missouri residents with renal transplants or with chronic renal insufficiency. The MoKP maintains an End Stage Renal Disease (ESRD) patient database, which currently contains over 13,000 patient records, of which over 2,500 are from active patients. The MoKP Patient Information Network is a WWW-based resource developed to streamline information exchange between ESRD treatment facilities and the MoKP. We have implemented a system for application and verification of digital signatures on new patient applications for services from the MoKP, which are submitted using the MoKP Patient Information Network.

Application. New patient applications to the MoKP involves collection of patient data (demographics, treatment, insurance and benefits) via interview by a trained social worker, who then submits compiled information to the Patient Information Network using a CGI-based form. Before implementation of the digital signature utility, the social worker was required to print off the completed application form, sign it, obtain the signature of the patient, and forward the signed forms to the MoKP by post. Our utility provides the means for both the social worker and the patient to digitally sign the completed application form at the time of electronic submission, thereby obviating delays in application processing. Moreover, the digital signature is evidence to authorized system users that the application truly was signed by the claimed signer, and thus provides a means of non-repudiation.

Conclusions. Our system utilizes widely available public key cryptographic methods implemented within a client/server JavaScript shell. To sign a document, the signer initiates the application of a secure hash algorithm to the document, thereby generating a document digest. A digital signature is then produced using the signer's private key and the document digest, using the mathematical techniques specified in the algorithm. Any individual with access to the signer's public key, the document, and the digital signature can verify the signature using the algorithm. Potential users of the system are assumed to have access to public keys. A signature that verifies correctly provides evidence that the owner of the public key signed the document, and that it has not been altered since it was signed. In our system, document metadata (*e.g.*, digital signatures, time stamps) are housed within a relational database. By storing documents and their signatures separately, our system allows the application of multiple signatures to each document, as well as storage and delivery of all document versions, a requirement for this particular application. Such methods should prove useful in development of user-friendly systems for local and remote delivery of diverse document types in health care environments. Use of these systems should enhance data integrity and streamline workflow in healthcare information applications.

Acknowledgments

This work was supported in part by grants LM07089 and LM05415 from the National Library of Medicine, and by the Missouri Kidney Program.

1091—8280/97/$5.00